International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 11
ISSN 2321-6905
November-2014

International Journal of Science Engineering and Advance Technology

Effective Data Hiding Method Through Pixel Pair Matching

N.Arjun[1], Ch.Sridevi[2], V.Dhana Raj[3], A.Praveen[4]
[1]M.TECH Scholar, [2]Assistant Professor, [3] Professor, [4] HOD Dept. of ECE
BVC Engineering college, Odalarevu, AP, India

Abstract:

This work proposes a new data-hiding method based on pixel pair matching , which is to use the values of pixel pair as a reference coordinate, and find a coordinate in the neighborhood set of this pixel pair based on the given message. Further the pixel pair is replaced by the searched coordinate to cover the digit. Two methods has been proposed to overcome this problem one is Exploiting modification direction (EMD) and another is diamond encoding (DE). The proposed methods offer lower distortion as compared to the existing methods by providing more compact neighborhood sets and allowing embedded digits in any notational system.

Key words- distortion, data hiding, compact neighborhood,

INTRODUCTION:

DATA hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are termed as cover images and images with data embedded are termed as stego images. After embedding, pixels of cover images will be modified and distortion occurs. The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload.

The least significant bit substitution method, referred to as LSB in this paper, is a well-known data-hiding method. This method is easy to implement with low CPU cost, and has become one of the popular embedding techniques. However, in LSB embedding, the pixels with even values will be increased by one or kept unmodified. The pixels with odd values will be decreased by one or kept unmodified. Therefore, the imbalanced embedding distortion emerges and is vulnerable to steganalysis. In 2004, Chan *et al.* Proposed a simple and efficient optimal pixel adjustment process (OPAP) method to reduce the distortion caused by LSB replacement. In their method, if message bits are embedded into the right-most LSBs of an m bit pixel, other m-r bits are adjusted by a simple evaluation. Namely, if the adjusted result offers a smaller distortion, these m-r bits are either replaced by the adjusted result or otherwise kept unmodified.

The LSB and OPAP methods employ one pixel as an embedding unit, and conceal data into the right-most LSBs. Another group of data-hiding methods employs two pixels as an embedding unit to conceal a message digit in SB a B-ary notational system. We term these data-hiding methods as pixel pair matching (PPM). In 2006, Mielikainen proposed an LSB matching method based on PPM. He used two pixels as an embedding unit. The LSB of the first pixel is used for carrying one message bit, while a binary function is employed to carry another bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance a pixel value has to be changed by one yet another 1/4 chance no pixel has to be modified.

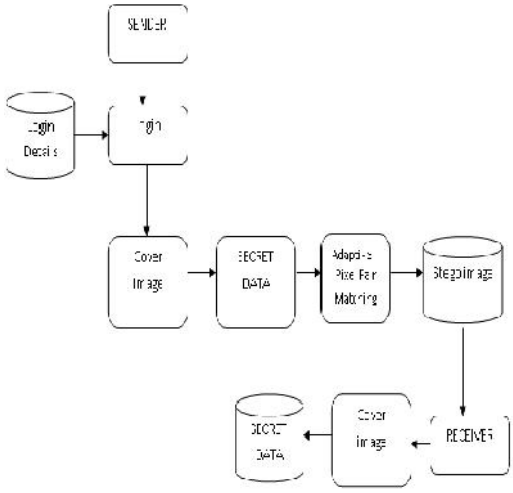
LSB matching and EMD methods greatly improve the traditional LSB method in which a better stego image quality can be achieved under the same payload. However, the maximum payloads of LSB matching and EMD are only 1 and 1.161 bpp, respectively. Hence, these two methods are not suitable for applications requiring high payload.

The embedding method of LSB matching and EMD offers no mechanism to increase the payload. In 2008, Hong [11] presented a data-hiding method based on Sudoku solutions to achieve a maximum payload of ½ $\log_2 9$ bpp. In 2009, Chao *et al.* Proposed a diamond encoding (DE) method to enhance the payload of EMD further. DE employs an

extraction function to generate diamond characteristic values (DCV), and embedding is done by modifying the pixel pairs in the cover image according to their DCV's neighborhood set and the given message digit. Chao used an embedding parameter to control the payload, in which a digit in a **B**-ary notational system can be concealed into two pixels, Where, $B = 2k^2+2k+1$, If, K=1 , i.e.=5 digits in a 5-ary notational system are concealed, the resultant payload is equivalent to EMD. If k=2 , B=13 ,if k=3,B=25. Note that is significantly increased as is only increased by one. Instead of enhancing the payload of EMD, Wang *et al.* [13] in 2010 proposed a novel section-wise exploring modification direction method to enhance the image quality of EMD. Their method segments the cover image into pixel sections, and each section is partitioned into the selective and descriptive groups. The EMD embedding procedure is then performed on each group by referencing a predefined selector and descriptor table. This method combines different pixel groups of the cover image to represent more embedding directions with less pixel changes than that of the EMD method. By selecting the appropriate combination of pixel groups, the embedding efficiency and the visual quality of the stego image is enhanced.

Another group of rather practical data-hiding methods considers security as a guiding principle for developing a less detectable embedding scheme. These methods may either be implemented by avoiding embedding the message into the conspicuous part of the cover image, or by improving the embedding efficiency, that is, embed more messages per modification into the cover. The former can be achieved, for example, using "the selection channel" such as the wet paper code proposed by Fridrich *et al*. The latter can be done by encoding the message optimally with the smallest embedding impact using the near-optimal embedding schemes. In these methods, the data bits were not conveyed by individual pixels but by groups of pixels and their positions.

This paper proposes a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency. The image quality obtained by the proposed method not only performs better than those obtained by OPAP and DE, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.



Architecture

MODULES:

- Extraction Function and Neighborhood Set
- Embedding Procedure
- Extraction Procedure
- Statistical Analysis of the Histogram Differences

Optimal Pixel Adjustment Process (OPAP)

The OPAP method proposed by Chan *et al.* in 2004 greatly improved the image distortion problem resulting from LSB replacement. The OPAP method is described as follows. Suppose a pixel value is *v*, the value of the right-most **r** LSBs of . Let be the pixel value after embedding message bits using the LSB replacement method and be the decimal value of these message bits. OPAP employs the following equation to adjust so that the embedding distortion can be minimized

$$v'' = \begin{cases} v' + 2^r, & v^{(r)} - s > 2^{r-1} \text{ and } v' + 2^r \leq 255 \\ v' - 2^r, & v^{(r)} - s < -2^{r-1} \text{ and } v' - 2^r \geq 0 \\ v', & \text{otherwise} \end{cases}$$

Where v'' denotes the result obtained by OPAP embedding. Note that v'' and v' have the same right-most *r* LSBs and thus, the embedded data can be extracted directly from the right-most *r* LSBs. Here is a simple example. Suppose a pixel value

$v^{(3)} = 000_2 = 0$ and $v^{(3)} - s = 0 - 5 <$

v=160=101000002 and the bits to be embedded are 1012. In this case,*r*=3 and *s*=5 . After is embedded, we obtained $v' = 165.$. Because we obtained $v'' = v' - 2^3 = 165 - 8 = 157 = 10011101_2$. Thus, after embedding 101_2, the pixel value 160 is changed to 157. To extract the embedded data, we simply extract the right-most three LSBs of 157.

Extraction Function and Neighborhood Set:

The definitions of $\Phi(x, y)$ and *f(x, y)* significantly affect the stego image quality. The designs of $\Phi(x, y)$ and *f(x, y)* have to fulfill the requirements: all values of *f(x,y)* in $\Phi(x, y)$ have to be mutually exclusive, and the summation of the squared distances between all coordinates in $\Phi(x, y)$ and (x,y) has to be the smallest. This is because, during embedding (x,y), is replaced by one of the coordinates in $\Phi(x, y)$. Suppose there are B coordinates in $\Phi(x, y)$, i.e., digits in a B-ary notational system are to be concealed, and the probability of replacing (x,y) by one of the coordinates in $\Phi(x, y)$ is equivalent. The averaged MSE can be obtained by averaging the summation of the squared distance between (x,y) and other coordinates in $\Phi(x, y)$. Thus, given a $\Phi(x, y)$, the expected MSE after embedding can be calculated by

$$\mathrm{MSE}_{\Phi(x,y)} = \frac{1}{2B} \sum_{i=0}^{B-1} \left((x_i - x)^2 + (y_i - y)^2 \right)$$

Embedding Procedure:

Suppose the cover image is of size $M \times M$, is the message bits to be concealed and the size of S is $|S|$. First we calculate the minimum B such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input: Cover image of size , secret bit stream , and key Kr .

Output: Stego image I',CB , , and Kr.

1. Find the minimum B satisfying, and Convert S into a list of digits with a B-ary notational system SB .

2. Solve the discrete optimization problem to find CB and

3. In the region defined by $\Phi_B(0, 0)$ record the coordinate such that \ $f(\hat{x}_i, \hat{y}_i) = i, 0 \leq i \leq B - 1$..

4. Construct a non repeat random embedding sequence Q using a key Kr .

5. To embed a message digit SB, two pixels (x,y) in the cover image are selected according to the embedding sequence Q, and calculate the modulus distance $d = (s_B - f(x, y)) \bmod B$ between and , then replace (x,y) with .

6. Repeat Step 5 until all the message digits are embedded.

Comparison of Experimental Results:

Six images Lena, Jet, Boat, Elaine, Couple, and Peppers, each sized 512* 512, are taken as test images to compare the MSE obtained by APPM, OPAP, and DE. The payloads were set to 400 000, 650 000, and 1 000 000, respectively. Message bits were generated by using a pseudorandom number generator (PRNG). The results are shown in Tables IV–VI.

Tables IV–VI reveal that the performance of the proposed APPM method is the best under various payloads. For example, with the payload 400 000 bits, the averaged MSE of 2-bit OPAP is 1.244, whereas the averaged MSE of DE is 0.887. However, the proposed method has the smallest averaged MSE, 0.640. For larger payload, such as 650 000 and 1 000 000 bits, the proposed method also performs better than OPAP and DE because APPM selects the smallest notational system that provides just enough embedding capacity to accommodate the given payload with the least distortion.

TABLE V
MSE COMPARISON (Payload = 650 000 bits, 2.480 bpp)

Image	3-bit LSB	3-bit OPAP	DE (k=3)	APPM ($c_{32}=7$)
Lena	8.653	4.543	3.154	2.604
Jet	8.638	4.542	3.164	2.609
Boat	8.674	4.552	3.170	2.598
Elaine	8. 728	4.555	3.163	2.582
House	8.871	4.546	3.169	2.600
Sailboat	8.708	4.534	3.159	2.610
Average	8.712	4.545	3.163	2.601

TABLE VI
MSE COMPARISON (Payload = 1 000 000 bits, 3.815 bpp)

Image	4-bit LSB	4-bit OPAP	DE (k=10)	APPM ($c_{159}=37$)
Lena	40.531	20.457	17.991	16.106
Jet	40.530	20.457	18.051	16.113
Boat	40.539	20.527	20.365	16.112
Elaine	40.530	20.498	18.052	16.104
House	40.596	20.456	18.096	16.102
Sailboat	40.583	20.482	19.227	16.108
Average	40.551	20.479	18.63	16.108

CONCLUSION

This paper proposed a simple and efficient data embedding method based on PPM. Two pixels are scanned as an embedding unit and a specially designed neighborhood set is employed to embed message digits with a smallest notational system. APPM allows users to select digits in any notational system for data embedding, and thus achieves a better image quality. The proposed method not only resolves the low-payload problem in EMD, but also offers smaller MSE compared with OPAP and DE. Moreover, because APPM produces no artifacts in stego images and the steganalysis results are similar to those of the cover images, it offers a secure communication under adjustable embedding capacity.

REFERENCES:

[1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[2] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, pp. 727–752, 2010.

[4] T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in *Proc. SPIE, Media Forensics and Security*, 2010, vol. 7541, DOI: 10.1117/12.838002.

[5] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 1, pp. 111–119, Mar. 2006.

[6] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Int. Workshop on Multimedia and Security*, 2001, pp. 27–30.

[7] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognit.*, vol. 37, no. 3, pp. 469–474, 2004.

[9] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.

[10] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.

[11] W. Hong, T. S. Chen, and C. W. Shiu, "A minimal Euclidean distance searching technique for Sudoku steganography," in *Proc. Int. Symp. Information Science and Engineering*, 2008, vol. 1, pp. 515–518.

[12] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.